

NOTE: Protective Measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a different alert level.

Action Number	Checklist		ORANGE - HIGH (HIGH RISK of terrorist attack) Recommended Protective Measures:
	Yes	No	
O-1			Disseminate the ORANGE advisory and share pertinent information related to the Homeland Security Threat Condition with state agencies/offices and government officials.
O-2			Continue all measures listed in the Homeland Security Threat Condition GREEN, BLUE and YELLOW Advisories.
O-3			Activate the agency's Emergency Operations Center (EOC) for an initial situation briefing of EOC staff and government officials. Following the initial briefing maintain staffing, as appropriate.
O-4			Place all emergency management and specialized response teams on full alert status, as appropriate.
O-5			Review critical infrastructure and facility security plans and adjust accordingly. Possible security recommendations or considerations include: <ul style="list-style-type: none"> • Limiting access points to critical infrastructure facilities to the absolute minimum, and strictly enforcing entry control procedures. Locking all exterior doors except the main facility entrance(s). Identifying and protecting all designated vulnerable points. • Searching all suitcases, briefcases, packages, etc. brought into a facility. • Checking all visitors' purpose, intent and identification. Checking that contractors have valid work orders outlining tasks to be performed within the secured facility. Requiring a visitor's sign-in log with information from their identification. Escorting visitors when they are in the facility, until they leave. Checking where the visitors were or worked to assure nothing is amiss or left behind. • Keeping critical response vehicles in a secure area or in an indoor facility. Keeping garage doors closed except for bona fide needs. • Enforcing parking of vehicles away from sensitive buildings. Erecting barriers and obstacles to control the flow of traffic, as appropriate. Visually inspecting the interior and undercarriage of vehicles entering parking lots and terraces. • Increasing defensive perimeters around key structures and events. Increasing security patrols around critical infrastructure facilities. Contacting allied government agencies within the jurisdiction and advising them of the need for increased security and awareness. • Coordinating closure of public roads and facilities that might make critical facilities more vulnerable to attack.
O-6			Determine if personal protective equipment (PPE) and specialized response equipment has been checked, issued, and readily available for deployment, if applicable.
O-7			Suspend public tours of critical infrastructure facilities. Limit access to computer facilities.
O-8			Increase monitoring of computer and network intrusion detection systems and security monitoring systems. Determine if sufficient technical resources are available to respond to and mitigate a cyber attack.